Some Papers on the Theory of Numbers.

By Arthur S. Hathaway, *Johns Hopkins University.*

The principles upon which the following papers are founded were developed while attending the Lectures of Professor Sylvester on the Theory of Numbers, in 1879–80; and were presented before the Mathematical Seminary in May, 1880, Jan., Feb., March, 1881. The death of my wife, who had shared with me in the work, and the professional duties of a stenographer, left neither opportunity nor inclination to make a more extended publication of them. Feeling confident, however, that the principles were of value in simplifying the Theory of Numbers, I returned to the subject in the beginning of the present year (1884). It is due to Professor Sylvester to state that the beginnings of my knowledge in the Theory of Numbers were obtained entirely from short-hand notes of his lectures; and that it was his suggestive presentation of the Theory of Congruences that led to the development of these principles.

The first paper, while it is introductory to, is intended to form a part of the second paper. The latter paper is founded upon an extension of the idea of division, which permits the consideration of any dividend whatever. Subjects which are ordinarily considered only in the general theory of Ideal Primes can thus be treated much more simply; and so naturally is one led to the necessary treatment, that I arrived at the solutions of the principal problems of these subjects without any knowledge of the theory of Ideal Primes. An example is the resolution of cyclotomic functions with respect to a prime modulus not only, which lies at the foundation of Kummer's theory of Ideal Primes, but with respect to a power of a prime.

I.—On Integer Classes.

There is a marked similarity between the ideas of Divisibility and Evanescence, which is exemplified in the three fundamental principles of division, viz.:

1st. If two terms are separately divisible, so is their sum and difference.

2d. If a term is divisible, so is a multiple of it.

3d. If a product is divisible and one factor is neither divisible nor *partially* divisible (*i. e.* relatively prime to the divisor), then the remaining factor is divisible.

The last principle is of the same utility in the Theory of Congruences as is the corresponding one in the Theory of Equations; and what happens in the former theory would have its analogue in the latter if it dealt with *partial* zeros.

The combination of the second and third principles leads to a fundamental proposition connecting different divisors, viz. that if a term is divisible by several relatively prime divisors, it is divisible by their product; while the combination of the first and second leads to another fundamental proposition which furnishes the basis of a method for utilizing the similarity above noticed, viz., any combination of sums and products of terms retains its remainder with respect to a given divisor, no matter how the several terms of the combination be replaced by others having the same remainders. That is to say (grouping together as a *class* all terms which have the same remainder), the results of any combination of sums and products of classes constitute members of one and the same class. Here we mean, for example, by the product of two classes, the assemblage of all possible products between the terms of the two. We are thus led to consider a class as a molecular body, as it were, any portion of which identifies the whole.

What corresponds to division among the classes is the theory of the linear congruence, in the ordinary sense, or as it will be here termed, of the linear modular equation $AX=B$. The problem for solution is a special one, limiting us to the question whether any of the given classes satisfy this modular equation, which is not answered by the symbolic solution $\frac{B}{A}$. The performance of the division here indicated might be presumed, in general, not to give rise to integers; although if, and only if there are integers resulting, is there a solution in the restricted sense which confines us to the consideration of integers only. The application of the third principle to the determination of the maximum number of solutions (by the substitution of two solutions, precisely as in the Theory of Equations) naturally excludes from general consideration the case where A is a divisible or partially divisible class (or, as it might legitimately be called, a *zero*, or *partially zero* class). With this exclusion, linear modular equations are shown to have but one solution. That the solution is not merely symbolic, but actually one of the given classes, is due to the distinctive feature that the number of classes is finite, and not infinite, so that AX, A multiplying successively all the

classes X, and giving rise each time to different classes B, must repeat all the classes over again. There are several important consequences of this feature.

First, is the linear relation among any relatively prime integers, $k_1, k_2, \ldots$, that the equation

$$\frac{k_1 k_2 \ldots}{k_1} x_1 + \frac{k_1 k_2 \ldots}{k_2} x_2 + \ldots = 1$$

is soluble in integers. Second, is the property that successive involutions of a class must finally bring it into some class whose powers repeat itself. These, which have been called repetents,* are *zero*, *unity*, and, for composite moduli, various *partial zeros*. Third, is the existence of cycles of classes, defined by the property that the members of a cycle are repeated over again in some order when severally multiplied by any one member of the cycle. An important example is the cycle composed of all classes which are relatively prime to the modulus.

It is worthy of note that this definition secures the property within the cycle, that quotients are one valued without reference to the restriction of the third principle; and it would be perfectly proper to treat cycles upon this supposition. The properties of cycles may be developed, however, from the definition alone, *ab initio*, whatever the nature of the terms with which we deal. The following are a few of the immediate deductions from the definition, the more general properties being reserved for a future paper:

A cycle contains all the powers of its members, and, therefore, some repetents. If the multiplication of each member of a cycle by a given term leave one member unaltered, it will leave all unaltered; for we may first exhibit (by multiplication) the unaltered member as a factor of all, and then perform the multiplication. If the multiplier is a member it does not alter itself, and is therefore a repetent. Any member raised to the power represented by the number of members is a repetent; for it leaves the product of all the members (which is a member) unaltered. All the repetents of a cycle are equal, since either of two is the same as their product. Every member is repeated as many times as is the repetent, and conversely; for, multiplying the terms of a cycle by a member exhibits it wherever there is a repetent; and multiplying by a power of the member which is one less than the number of members, exhibits the repetent wherever the member occurs.

* By Mr. Mitchell, in his article on Binomial Congruences, in Vol. III of this Journal.

A fourth consequence of this feature is a *form* into which a class may be thrown, which exhibits its relations to the classes which it determines with respect to the relatively prime factors of the modulus. It is well known that any class $Y(\text{mod. } k_1 k_2 \ldots)$ can be thrown, in one way, and one way only, into the form $\frac{k_1 k_2 \cdots}{k_1} X_1 + \frac{k_1 k_2 \cdots}{k_2} X_2 \ldots$, where $k_1, k_2, \ldots$ are relatively prime factors of the modulus; viz. X_i is the class (mod. k_i) which is the solution of $\frac{k_1 k_2 \cdots}{k_i} X_i = Y(\text{mod. } k_i)$. Denoting by Y_i the class determined by $Y(\text{mod. } k_i)$, and writing $h_i = \frac{k_1 k_2 \cdots}{k_i}$, the symbolic solution for X_i is $\frac{Y_i}{h_i}$; the use of which in the above form is legitimate, if we consider it in the restricted sense of denoting only the integral terms which occur in performing the indicated division. We may thus write:

$$Y = h_1 \frac{Y_1}{h_1} + h_2 \frac{Y_2}{h_2} + \ldots (H).^*$$

The value of this form consists in the fact that any combination of classes (Y), (mod. $k_1 k_2 \ldots$) is obtained by forming the same combination of corresponding arguments $(Y_i)(\text{mod. } k_i)$; as is evident on considering the way in which the arguments are derived from the class which the form represents. For the zero class the arguments are zeros; for the partial zeros, corresponding partial zeros; for the unit class the arguments are units; for repetents, the arguments are repetents; and if $k_1 k_2 \ldots$ each involves a single prime only, the arguments of the repetents are confined to zero and unity. Corresponding arguments of cycles are cycles.

The least power (index) for which λ becomes a repetent is the least common multiple of its indices with respect to the relatively prime factors of the modulus which is great enough to permit the partial zero arguments to become zero. In general, the form (H) renders visible, so to speak, the properties of a class in terms of its simultaneous properties with respect to the relatively prime factors of the modulus; and we see that it may be stated as a general principle that the number of classes which possess a property whose negation among the arguments

* Writing $h_i \frac{1}{h_i} = R_{k_i}$ we obtain a form which is given by Mr. Mitchell, R_{k_i} being his notation for the common solution of $x \equiv 0$, mod. h_i, $x \equiv 1$, mod. k_i. This common solution satisfies the definition of a repetent, $x^2 \equiv x$ (mod. $k_1 k_2 \ldots$) and also $R_{k_i} R_{k_j} \equiv 0$ (mod. $k_1 k_2 \ldots$); whence the property of the form $R_{k_1} Y_1 + R_{k_2} Y_2 + \ldots$ In the product of two such forms, for example, the cross products drop out, leaving only the products of corresponding arguments multiplied by the squares of the corresponding coefficients, which are repetents. It appears that a form possessing the same property is obtained by merely writing the symbolic solution for the variables X_i in a well-known form, which at once discloses the repetents and their properties.

involves its negation in the class, is the product of the number of classes possessing that property with respect to each of the relatively prime factors of the modulus. As examples are: the property of being relatively prime to the modulus; of containing the factors common to the modulus and a given number; of being n^{th} power residues of the modulus; of satisfying a given congruence with respect to the modulus.

What corresponds to evolution among the classes is the resolution of the Binomial congruence $X^n = A$. The n^{th} root of a class A gives rise in general only to surds; and if, and only if exact n^{th} powers occur in the class A, will there be a solution. Having found one solution, there is the same dependence upon the solutions of $X^n = 1$ for the others as in the Theory of Equations. The determination of the solvable equations of this sort constitutes the theory of n^{th} power residues; and for this, special methods have been invented, having no analogy to methods in the Theory of Equations; for example, the Theorems of Reciprocity.

So far as the theory of the general equation of the n^{th} degree is concerned, the substitution of $n+1$ solutions and elimination of coefficients, leads, precisely as in the Theory of Equations, to the conclusion that the product of the differences of $n+1$ solutions multiplied into each coefficient is a divisible quantity, so that for a prime modulus, the number of solutions cannot exceed the degree unless the modular equation is identical through the divisibility of each of its coefficients. The reciprocal of a solution cannot contain any factor of the modulus if the coefficient of X^n does not; so that modular equations which have no impossible or indeterminate solutions can be reduced to the standard form $X^n + A_1 X^{n-1} + \ldots A_n = 0$. In the further theory, we catch glimpses, for the most part as the result of special and disconnected methods, of similarity to the Theory of Equations. Equal roots $(X-A)^2$, for example, render the discriminant divisible, and common roots, the resultant. In the case of a prime modulus, Galois' Theorem furnishes a basis for what are called imaginary solutions, giving to a modular equation its complement of solutions. Investigators, however, have kept constantly before them the restriction that they were dealing with integers; a self-imposed restriction which is in nowise indicated by the fundamental principles of division, which only require that the *divisor* shall be an integer. This restriction is so vital that were it not for the *accident* of the theory that the number of integer classes is finite, even a linear equation would not have, in general, a solution. We may illustrate

this by reference to algebraic division, the theory of modular equations in which has not been developed. The residues of an integer algebraic function, though less than it in degree, are infinite in number.

In division and evolution, the fractions and surds were neglected, because there was no place for them. A true notion of division will give the fractions and integers which result from the division of one class by another a place together. The n surd n^{th} roots, and in general, the n roots of an algebraical equation of the n^{th} degree will have a place in n classes, connected by the same relations as the roots themselves. Some will fall in the integer classes; others will form new classes which contain no integers.

II.—General Theory of Division.

Having given a system of integers consisting of primes, their powers and products,* the idea of division confines us, in the first instance, to the system. But by confining our divisors to that system, the fundamental principles of division will permit the consideration of any terms whatever (roots of equations in the system) as dividends—the quotients being restricted, of course, not to involve the reciprocals of any divisors of the divisor.† The factors of a divisor are the partial zeros of its modular system. The reciprocals of these factors are the partial infinites; and unless they be excluded from general consideration, any quantity whatever can be made to contain the divisor.

On grouping together as a class all terms which have the same remainder, the integral system will fall either into an infinite or a finite number of classes; and there is a marked difference between the theory of division in these two cases. For example, if the number of classes is infinite, the results of division

* It is necessary for the existence of the first principle that the integers of the system should repeat themselves by addition and subtraction; and for the existence of the third principle that the resolution of an integer into products of powers of primes should be possible in only one way.

† While this notion of division is sufficiently definite so long as the dividend is an integer or a fraction, when we introduce irrational dividends, division by a prime say, is not exactly defined without regarding a root of the prime as a factor of it. The actual exhibition of an integer as a factor of an irrational quantity may be practically difficult. Thus, a root of $x^2 - 3x + 5$ is divisible by 5, a prime of the ordinary system, whose only factors are roots of 5; but we can substantiate this only theoretically, viz., the product contains 5, and since the square of the difference is relatively prime to 5, one root cannot contain $\sqrt[n]{5}$ and the other $\sqrt[m]{5}$. This conception of division which renders it no more difficult, theoretically, to consider irrational than rational quantities in the Theory of Numbers, was forced upon me, in developing the analogy between equations and congruences. I had defined $f^{-1}(a)$ as a solution of $f(x) \equiv a \bmod. k$, and shown that its ordinary combinations also held (mod. k); also that $f^{-1}(a + \lambda k)$ was a solution, and gave all the integral solutions. Then defining $f^{-1}(a)$ as imaginary (mod. k), if variations of a by λk gave no integers, I was led to define k times an imaginary quantity as $\equiv 0 \bmod. k$.

between two classes will not, in general, involve integers, the quotients being entirely fractional. Only if there exist among relatively prime factors of the modulus the relation that $h_i x + k_i y = 1$ is soluble in integers, may every class be thrown into the form (H). As in this case, there exist repetents other than zero or unity, the modulus must be a divisor of one or more terms of the form $x^2 - x$, where x is its residue. There is no modular equation of finite degree which is satisfied for every integral class and only for such, by means of which we may satisfy ourselves whether a root of a given equation determines an integral class or not; but if a modular equation be written in the standard form, and the solution is integral, the coefficients must be integral, and the solution a divisor of the constant term.

There is yet an unsettled question in the extension of the notion of division to any dividend whatever, viz., what is the relation as to divisibility between the modulus and any of its roots. In other words, what are the roots of the zero class? If we assume them to be the zero class itself, we make no distinction between division by an integer and any of its powers or roots. We practically *group* the powers and roots of a prime together, and the assertion that a given dividend contains k, merely asserts that it contains some one out of the products of the groups which the prime factors of k determine. We are only sure, for example, if the dividend is integral, that it contains some integral powers of these primes. Observe that we have arranged the system of divisors consisting of primes, their powers and roots into a system consisting of *group* primes $[p]$ and their products, the powers and roots of any one of which repeat itself. With such a system of divisors it is evident that roots of the zero class are zero; and when the modulus is a prime group, the correspondence with the Theory of Equations is exact. The more general supposition is that roots of the zero class are zeros or partial zeros, so that the modular equation $X^n = 0$ does not have all of its roots equal. We thus have the peculiarity of an infinite number of partial zeros for a modulus $p^i q^j$, arranged, however, in a finite number of relatively prime groups, $[p]$, $[q]$ . . .

The determination of the arbitrary variable of a function

$$f(x) \equiv x^n + a_1 x^{n-1} + \ldots a_n,$$

so that $f(x)$ shall be divisible by a given modulus k is one and the same thing with seeking the solutions of the infinite number of equations embraced in the modular equation $X^n + A_1 X^{n-1} + \ldots A_n = 0$, where $A_1, \ldots A_n$ are the classes

with respect to the modulus k which are determined by $a_1, \ldots a_n$. For, since these equations differ only by algebraic terms which identically contain k, a root of any one when substituted in any other, $f(x)$, for example, renders it divisible by k; and if β be a quantity which substituted in $f(x)$ renders it divisible by k, then β is a root of one of these equations, viz. $f(x) - f(\beta) = 0$.

We now seek the number of classes which satisfy a modular equation of the n^{th} degree, not by the substitution of $n+1$ solutions, the result of which has been already pointed out, but by a more direct method. The roots of $f(x) = 0$ determine n classes, $X_1 = \alpha_1 + \lambda_1 k$, $X_n = \alpha_n + \lambda_n k$. On the other hand these classes determine a modular equation $(X - X_1) \ldots (X - X_n) = 0$, which includes $f(x) = 0$, and an infinite number of equations which differ from it by identical multiples of k. They are therefore contained in $X^n + A_1 X^{n-1} + \ldots A_n = 0$; but conversely, β being a root of one of these latter equations, it simply renders $f(\beta)$ divisible by k, which may be through distribution of the factors of k among the terms of the product $(\beta - \alpha_1) \ldots (\beta - \alpha_n)$ so that not a single factor shall contain k. The quantity β will not then be found among the classes $X_1 \ldots X_n$ and the first modular equation will not contain all the equations of the latter. We may state the matter in this way: among the equations $f(x) + k\phi(x) = 0$, certain forms of $\phi(x)$ correspond to the equations determined by the roots of one, $f(x) = 0$; and the different sets of such forms correspond to different ways of separating the modular equation into linear modular factors.

As to the possibility of a multiplicity of ways, it depends upon the possibility of finding a quantity β which shall be common to two classes $\alpha_1 + h_1\lambda_1$, $\alpha_2 + k_1\lambda_2$, where h_1, k_1 are relatively prime factors of k; that is to say, upon the possibility of the solution of $h_1\lambda_1 - k_1\lambda_2 = \alpha_2 - \alpha_1$; λ_1, λ_2 not involving the reciprocals of factors in k_1, h_1. This is possible if $h_1 x - k_1 y = 1$ is soluble in integers; and the form (H) then gives the common terms $\beta + \lambda h_1 k_1$ from the arguments consisting of any two solutions of the modular equation with respect to h_1, k_1 as moduli. In case, therefore, the system of integers is such that the number of classes with respect to any modulus is finite, the solution of modular equations is made to depend upon their solution with respect to the relatively prime factors of the modulus.

The number of solutions, as has already been pointed out, is then the product of the number of solutions with respect to each relatively prime factor of the modulus. The like may be shown with respect to the resolution of a function into modular factors, by an extension of the form (H). Thus, if $f_i(X)$

denote the modular function determined by $f(x)$ mod. k_i, then $f(X) = h_1 \frac{f_1(X)}{h_1} + h_2 \frac{f_2(X)}{h_2} + \ldots$ mod. $k_1 k_2 \ldots$ As an example, if $f_1(X) = A.B$ mod. k_1, $f_2(X) = C$ mod. k_2 $\therefore f(X) = \left(h_1 \frac{A}{h_1} + h_2 \frac{1}{h_2}\right)\left(h_1 \frac{B}{h_1} + h_2 \frac{C}{h_2}\right)$

$$= \left(h_1 \frac{B}{h_1} + h_2 \frac{1}{h_2}\right)\left(h_1 \frac{A}{h_1} + h_2 \frac{C}{h_2}\right) \text{ mod } k_1 k_2.$$

Confining our attention now to powers of primes as moduli, the factors of the modulus are its roots; and if these can be distributed among two or more factors $\beta - \alpha_1$, $\beta - \alpha_2$ of $f(\beta)$, which is, as we have seen, the necessary and sufficient condition that $f(X)$ shall be resoluble into linear modular factors in more than one way, then the differences, $\alpha_2 - \alpha_1$ of these factors will also contain a root of the modulus. Therefore the product of all differences, or the discriminant of $f(x)$ will contain some root of the modulus. The discriminants of all the equations of a modular equation belong of course to the same class, since they are rational functions of the coefficients. Therefore, if the discriminant of a modular equation is relatively prime to the modulus, it cannot be resolved in more than one way into linear factors. On the contrary, if the discriminant contain a factor of the modulus, the modular equation is resolvable into linear factors in an infinite number of ways. Suppose, for example, that $\alpha_1 - \alpha_2 = \mu_2 p^{y_2}$, $\ldots$ $\alpha_1 - \alpha_r = \mu_r p^{y_r}$, where y_2, y_r are quantities greater than zero, arranged, we will suppose, in ascending order of magnitude. Then if $\beta = \alpha_1 + \lambda p^{i_1}$, $f(\beta) = \lambda p^{i_1} (\lambda p^{i_1} + \mu_2 p^{y_2}) \ldots (\lambda p^{i_1} + \mu_r p^{y_r}) Q$. In order that p^i may be a divisor of $f(\beta)$, it is evident that i_1 cannot be less than $\frac{i}{r}$, since in making up i, we must take the least exponent i_1, y_s in each of the above factors. The suppositions $i_1 = y_s$ are included in $\beta = \alpha_s + \lambda p^{i_s}$. If $\frac{i}{r}$ fall between y_s and y_{s+1}, the least value of i_1 is the first of the series $\frac{i - \sum_2^{s'} y_s}{r - s' + 1}$, $s' \geqq s$, which falls between $y_{s'}$ and $y_{s'+1}$, and the same for i_s. Notice that $i_1 = \frac{i}{r}$ if $\frac{i}{r} \leqq y_2$. The values of β which render $f(\beta)$ divisible by p^i are therefore of the forms $\alpha_1 + \lambda p^{i_1} + \mu p^i$, $\ldots$ $\alpha_n + \lambda p^{i_n} + \mu p^i$; and we call attention to the fact that when the discriminant contains a factor of the modulus, n values of β whose differences are relatively prime to the modulus cannot be found. If we make no distinction between division by the modulus and any power or root of it, these forms (which consist of groups of classes corresponding to variations of the parameter λ) reduce to members of the classes

determined by $\alpha_1, \ldots \alpha_n$, of which those determined by the cognate roots $\alpha_1 \ldots \alpha_r$, for example, are equal. The modular equation is then resolvable into linear factors in only one way, and involves equal factors.

This notion of division, which it is useful to introduce when considering a function with respect to those exceptional divisors of it which are divisors of its discriminant, does not determine the actual divisor to be p^i, but, as already pointed out, only locates it among the group $[p]$, consisting of the powers and roots of p^i. Such an hypothetical division leads, however, to certain definite results with regard to actual division by p. Namely: (1) in the determination of the integer classes which render $f(x)$ divisible by some p^α, we are sure that the integers of those classes render it divisible by p; (2) in establishing that one algebraic function divides another for some p^α as modulus, we are sure that α will be at least $= 1$, for, we may proceed by actual division with respect to the modulus p until we get a residue of the divisor, which must identically contain some p^α, and therefore p, since the coefficients are integral.

The general method for determining whether or not the class pertaining to a given quantity is integral, is to substitute it in the one or more modular equations whose solutions are known to be integral, and which include among their solutions every integral class.

The number of integer residues of a prime modulus p being π, we have such a modular equation in

$$X^\pi - X = 0 \text{ (mod. } p). \qquad (P)$$

For, excluding the zero class, the remaining classes satisfy $X^{\pi-1} = 1$, since they form a cycle; and the differences of all the classes being relatively prime to p, so is the discriminant of (P). The integral classes are therefore the complete solutions of (P).

With respect to p^i as modulus, we have a set of such modular equations,

$$X^\pi - X = Rp \text{ (mod. } p^i) \qquad (R)$$

where R is an integral class (mod. p^{i-1}). For, by (P), every integer satisfies an equation of the form $x^\pi - x = rp$, and therefore every integral class (mod. p^i) satisfies one or other of the modular equations (R) determined by these equations. Also, each modular equation (R) has only π solutions, since its discriminant is relatively prime to p; and the whole number of such modular equations is $\pi^{i-1} =$ the number of ways of filling $\lambda_1 p^{i-2} + \ldots \lambda_{i-1}$ with residues of p. The π^i integral classes are therefore the complete solutions of (R).

Since the integers, if any, which render $f(x)$ divisible by p^i are obtained, if the discriminant is relatively prime to p, by adding multiples of p^i to the roots of $f(x)=0$, the substitution of these roots in the modular equations (R) determines whether this is possible. If, however, the discriminant contains p, such integers may be obtained by adding to some of the roots multiples of less powers of p; for example, by adding to one of the cognate roots $\alpha_1, \ldots \alpha_r$ multiples of p^{i_1}, where i_1 has a least value less than i and $\geq \frac{i}{r}$. This renders it necessary to consider the possibility of a quantity α_1 becoming an integer by the addition of (restrictedly) a multiple of a fractional power of p.

This is possible only when α_1 is one of a set of cognate roots of an irreducible integral equation whose discriminant contains p. For, if an integer $\beta=\alpha_1+\lambda p^a$, then $f(\beta)=\lambda p^a(\lambda p^a+\alpha_1-\alpha_2)\ldots(\lambda p^a+\alpha_1-\alpha_n)$; and contains restrictedly p^a, if $\lambda, \alpha_1-\alpha_2, \ldots \alpha_1-\alpha_n$ are each relatively prime to p; while, since $f(\beta)$ is rational, this must be an integral power of p. By application of the same principle that $f(x)$ is a (permissible mod. p) rational function of x, various restrictions upon the possible values of α may be obtained upon the supposition that $\alpha_1 \ldots \alpha_r$ is a set of cognate roots.

A striking restriction is that a *fractional* value of α is its *maximum* limit. For, if $\alpha_1+\mu p^{a'}=$ integer $(a'>\alpha=$ fraction), then the difference $\mu p^{a'}-\lambda p^a=$ integer, which is therefore divisible by some power of p between α' and α; but this is impossible, since λ is relatively prime to p. Thus, for example, if the roots of $f(x)=0$ become integers by additions of fractional powers of a divisor, p, of its discriminant, $f(x)$ will not be rationally divisible by unlimited powers of p; for we have simply to take i great enough so that $i_1, \ldots i_n$ are greater than these fractional powers, in order to determine a power p^i which is not such a divisor.

It is not necessary, however, that α should take a fractional value in order to have a maximum; for, α being an integer, the variations of λ by integer additions give all integers of the form $\beta+np^a$; and if we can determine the integer n so that $\lambda+n=M[p]$ and so increase α, λ pertains to an integral class mod. $[p]$. Therefore we can form from an integer β, and a non-integral quantity λ, mod. $[p]$, quantities $\alpha_1=\beta-\lambda p^{n_1}$ such that the integer n_1 is a maximum value of α.

The quantities λp^a which added to the roots of $f(x)=0$ give an integer β are given by the integral equation $f(\beta-\lambda p^a)=0$. On removing from this the factors p, the coefficients of powers of λ greater than the r^{th} must contain p,

since the $n - r$ solutions of λ corresponding to the roots outside the cognate set must be partial infinites (mod. p). Also similarly, as many of the coefficients of powers of λ which are $\leqq r$ will contain p as there are roots in the cognate set whose maximum powers of p for additions of which they become $= \beta$ are $< \alpha$. The remaining values of λ (mod. $[p]$) are obtained from the equation which results from dropping such coefficients; and according as a solution is or is not integral mod. $[p]$ can α be increased or not for a corresponding root of the cognate set. A particular case is $r = 1$; when the resulting equation is linear, and has always integral solutions. In other words, if $f(x)$ is rationally divisible by p, corresponding to a root of $f(x) = 0$ which has no cognates, mod. $[p]$, it is rationally divisible by unlimited powers of p, corresponding to that root.

In order that a quantity may become an integer by additions of some power of p, it is necessary and sufficient that it should satisfy $(P) = 0$ mod. $[p]$. This modular equation may be replaced by an infinite series with respect to the modulus p, viz.: $X^{\pi^i} - X^{\pi^{i-1}} = 0$ mod. $p \ldots (P_i)$.
Since we can fill the form for the residues of p^i in $\pi^{i-1}(\pi - 1)$ ways so as to be relatively prime to p, this is the modular equation which is satisfied (mod. p^i) by every integral class;* but its discriminant, therefore, contains p. In fact, from the distributive property of the power π over a sum or difference (mod. p), $P_i \equiv P_1^{\pi^{i-1}}$ (mod. p). All solutions of (P_i) are therefore of the form $\beta + \lambda p^{\frac{1}{\pi^{i-1}}}$ where β is an integer; which includes, primitively, all quantities which can become integers by additions of p^α, α lying between $\frac{1}{\pi^{i-1}}$ and $\frac{1}{\pi^{i-2}}$. The solutions of (P_1) include the cases $\alpha \geqq 1$.

We may illustrate the preceding theory by the determination of the divisors of the cyclotomic functions. Take, for example, $f(x) \equiv x^4 - x^3 - x^2 - 2x + 4$, whose roots are $\phi(\rho) \equiv \rho + \rho^4 + \rho^{16}$, ρ being a primitive 21st root of unity. The powers of ρ for which $\phi(\rho)$ remains unchanged, which necessarily form a cycle mod. 21, are 1, 4, 16. If a prime p is a divisor, $\phi(\rho)$ must satisfy $x^p \equiv x$ mod. p; or since the power p is distributive mod. p, and the coefficients of ϕ integral,

$$\phi(\rho^p) \equiv \phi(\rho) \text{ mod. } p. \qquad (1)$$

The first member becomes identically the second if $p \equiv 1, 4, 16$, mod. 21; which determines forms of primes which are divisors of $x^4 - x^3 - x^2 - 2x + 4$, for

*The form of this modular equation (mod. p^i) shows that any set of incongruous classes (mod. p), raised to the π^{i-1} power, are the solutions of $(P) = 0$ (mod. p^i). If in the latter so resolved into linear factors, we substitute $X^{\pi^{r-1}}$ for X, we obtain a resolution of (P_r) mod. p^i into its non-cognate modular factors.

integral or (permissible) fractional values of x. For a prime p which is relatively prime to 21, and not one of these forms ($\equiv 1, 4, 16$, mod. 21), the first member of (1) is some root of the cyclotomic different from the second member; and if the congruence subsists, p is a divisor of the discriminant of $f(x)$. Conversely, for a divisor p of the discriminant of $f(x)$, this congruence subsists mod. $[p]$, but not necessarily mod. p. To obtain the primes, fractional powers of which <1 are added to the roots to make them integers, we seek the primitive solutions of $x^{p^i} - x^{p^{i-1}} \equiv 0$ mod. p. The solutions can only be primitive when p is a divisor of the index 21. The value of $i-1$ is the power of p which is contained in the index; and $\rho^{p^{i-1}}$ is a primitive $\left(\frac{21}{p^{i-1}}\right)^{\text{st}}$ root of unity $= \rho_1$. Thus if $\phi(\rho_1^r) \equiv \phi(\rho_1)$ mod. p is satisfied, p is a divisor of $f(x)$. Whence either $p \equiv 1, 4, 16$, mod. $\frac{21}{p^{i-1}}$, or p is a divisor of the discriminant of the cyclotomic corresponding to $\phi(\rho_1)$. We have evidently $\phi(\rho) \equiv \phi(\rho_1)$ mod. p, so that the cyclotomic corresponding to the first member is a power $= h$ of the cyclotomic corresponding to the second; and its roots are made integral by additions of a multiple of p^α, where α is some quantity conditioned by the inequality. Thus no power of p greater than $h^\alpha \frac{1}{h} \leq \alpha < \frac{1}{p^{i-2}}$, can be a divisor of $f(x)$. For example, $f(x)$ is divisible by 7, but not by 7^2.

The problem of the determination of the divisors of a function may be generalized, if instead of seeking the moduli for which a given function has a rational linear factor, we seek the orders of the rational modular divisors of a function with respect to a given modulus p^i. This more general problem we shall consider hereafter.

An important property of the π^{th} power is that it is distributive (mod. p) over a sum or difference. For, A and X being integral classes, so is $A + X$, so that $(A+X)^\pi = A + X = A^\pi + X^\pi$; therefore, the modular equation of $(\pi-1)^{\text{st}}$ degree, $(A+X)^\pi = A^\pi + X^\pi$ is *identical*, since it has π solutions (the integral classes) whose differences are relatively prime to the modulus.

This result leads to the conclusion that any system of integers such that the residues of a finite integer are finite in number consists of a factoring of ordinary integers;* for any prime p of such a system is contained in the ordinary binomial coefficients π, $\frac{\pi(\pi-1)}{1.2}$, . . . , and it readily follows that any integer is contained in the ordinary integer which represents the number of its residues. The number

* Ordinary integers are included in any system in the sense of representing repetitions of the unit of the system.

of residues of an integer may be called its *norm;* from which definition follows the property that the norm of a product is the product of the norms of the factors. We shall call the *least* ordinary integer which contains a given integer, its *subnorm;* from which definition follow the properties: The subnorm of a prime is an ordinary prime; of a power of a prime, an ordinary prime or a power of it; of a product, the least common multiple of the subnorms of the relatively prime factors. An ordinary prime is the subnorm of any of its factors. Those residues of a modulus which can be expressed as ordinary integers are precisely the ordinary residues of its subnorm. If a power n is distributive with respect to a modulus, the binomial coefficients $n, \frac{n.n-1}{1.2}, \ldots$ must contain the subnorm of the modulus. Hence, if we assume it as a property of these binomial coefficients, that they can have no ordinary common factor except a prime when n is a power of that prime, then, if, and only if the modulus is a factor of an ordinary prime will there exist distributive powers with respect to it, viz., the ordinary prime and its powers only. This theorem may be otherwise obtained as follows:

Firstly, n being a distributive power, it contains the modulus. The immediate consequence is that the discriminant $(n-1)^{n-1}$ of $X^n - X$ is relatively prime to the modulus. Secondly, n being a distributive power, the solutions of $X^n - X = 0$ repeat themselves by addition—*e. g.*, $(A+B)^n = A^n + B^n = A+B$. These conditions are sufficient, since we then have, with respect to each relatively prime factor (p^i) of the modulus as modulus, the *identity* $(1+X)^n = 1+X^n$, *i. e.*, it is satisfied by the n solutions of $X^n - X = 0$ whose differences are relatively prime to the modulus. Now, any ordinary residue of the subnorm of p^i is a solution (mod. p^i), viz., $1+1+\ldots = \lambda$; whence the subnorm must be an ordinary prime ν, since otherwise differences of the residues of ν would contain the prime factor of ν, and therefore the prime p. Again, each solution (mod. p^i) excepting zero, is relatively prime to p^i, and therefore its repetition gives rise to as many different solutions as there are ordinary integer residues of the subnorm ν; and if $1, X_2, \ldots X_s$ be a complete set of linearly independent solutions, any solution may be thrown in only one way into the form $\lambda_1 + \lambda_2 X_2 + \ldots \lambda_s X_s$, where $\lambda_1, \ldots \lambda_s$ are ordinary residues of ν. The whole number of solutions is therefore $\nu^s = n$; an equality which can only be possible for each relatively prime factor of the modulus when all have the same subnorm ν. Finally, if the subnorm of the modulus is an ordinary prime ν, then ν itself satisfies the two conditions of a distributive power; and as a consequence ν^s is a distributive power.

As we have seen, the norm of a prime modulus is a distributive power, and it is therefore a power of the subnorm. The preceding demonstration also shows, if $\nu^f = \pi$, that f represents the number of linearly independent residues of p. We shall use the term *degree*, in general, to signify the number of linearly independent residues. Depending upon the distributive property of the subnorm ν, is the proposition that if the degree of p is >1 there exist no primitive integral solutions of $X^{\pi^i} - X^{\pi^{i-1}} = 0 \text{ mod. } p^i$. For, α being an integer, we have successively, $\alpha^\pi = \alpha + Mp$, $\alpha^{\pi\nu} = \alpha^\nu + Mp^2$, . . . $\alpha^{\pi\nu^{i-1}} = \alpha^{\nu^{i-1}} + Mp^i$, so that every integral class satisfies a modular equation $X^{\pi\nu^{i-1}} - X^{\nu^{i-1}} = 0 \text{ (mod. } p^i)$ of less degree than that of the first modular equation, if $\pi > \nu$. Primitive solutions of this latter equation always exist in the special case $i = 2$, viz., $\alpha + \beta p$, β being relatively prime to p and α a primitive solution (including zero) for $i = 1$. If ν does not contain a power of p, primitive solutions always exist, namely, those for p^2. If, however, the *multiplicity* of p in ν is >1, every integral class satisfies ($i > 2$) a modular equation of this same form, of degree $\pi\nu^s$, $s < i - 1$, for which primitive solutions exist. In the case $\pi = \nu$, p being contained but once in ν, the residues of p^i are ordinary integers, and the primitive solutions are identical with those for ν^i. The number of primitive solutions is in the several cases $\pi^{i-2}(\pi - 1)\{\tau(\pi - 1) + 1\}$. The symbol τ coincides with the "totient of" except for $\pi = 2^f$, when there are no primitive solutions which are relatively prime to p unless the degree of the corresponding modular equation be still further reduced.

[TO BE CONTINUED.]